https://doi.org/10.5392/JKCA.2019.19.07.013

IoT 보안인증서비스 인증기준 중요도 우선순위에 관한 연구

A Study on Priority of Certification Criteria for IoT Security Certification Service

강다연*, 황종호**
경북대학교 경영학부 BK21플러스사업*, 동명대학교 경영정보학과**

Da-Yeon Kang(kdy2019@knu.ac.kr)*, Jong-Ho Hwang(jongho@tu.ac.kr)**

요약

사물인터넷(IoT) 제품 등의 보안이 허술해 각종 해킹 사고가 발생하고 있다. 보안위협을 막기 위해서는 기업이 먼저 보안수준이 높은 제품을 만들고 이용자도 안전한 제품을 선택하는 것이 무엇보다 중요하다. 이에 한국인터넷진흥원은 IoT제품 및 연동 모바일 앱의 보안을 시험하여 등급을 부과하고 있다. 보안인증서비스는 IoT 제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족 시 인증서를 발급해주는 서비스이다. IoT제품의 자율적 보안강화를 유도할 수 있고 국내 IoT기업 보안역량 강화 및 해외진출 활성화에 기여할 수 있으며, IoT제품에 대한 국민의 불안감 해소의 기대효과를 가질 수 있다. 본 연구에서는 IoT보안인증기준이 제시되어있지만 보다 강화해야 하는 평가 항목에 대한 중요도 우선순위를 도출하고자 한다. 이는 국내 사물인터넷기업 보안역량 강화 및 해외진출 활성화에 기여할 수 있는 가이드라인을 제시하는데 도움이 될 것이다.

■ 중심어 : | 사물인터넷 | 보안 | 우선순위 | 인증기준 | 보안위협 |

Abstract

Because security of Internet of Things(IoT) products and others is poor, there are many hacking incidents To prevent security threats, it is important for companies to first make products with high security levels and choose products that are safe for users. In response, the Korea Internet & Security Agency is testing the security of IoT products and linked mobile apps to impose ratings. Security certification service is a service that tests IoT products and linked mobile apps to ensure certain levels of security and issues certificates when they meet the criteria. It can induce autonomous security enhancement of IoT products, contribute to strengthening security capabilities of IoT companies in Korea and vitalizing their overseas advancement, and have the expected effect of resolving public anxiety over IoT products. In this study, the criteria for IoT security certification are presented, but the importance priority is sought to be derived for assessment items that need to be strengthened. This will help to provide guidelines that can contribute to strengthening the security capabilities of domestic Internet companies and boosting their overseas advancement.

■ keyword : | Internet of Things | Security | Priority | Certification Criteria | Security Threat |

접수일자 : 2019년 04월 17일
수정일자 : 2019년 05월 13일
심사완료일 : 2019년 05월 13일
교신저자 : 황종호, e-mail : jongho@tu.ac.kr

I. 서 론

정보기술의 발달에 따른 IT서비스의 다양화는 지금까지 경험해 보지 못한 보안문제 보장을 함께 요구하고 있다. 즉, 정보통신기술을 활용한 서비스 유형이 다양화됨에 따른 보안에 대한 대처문제를 의미한다. 예로 미국은 9.11테러발생 이후 마크 와이저(Mark Weiser)가 주창한 유비쿼터스 기술을 국가보안 문제의 허점을 보완하기 위한 수단으로 도입하여 자국 내 위험물품 반입을 사전차단하기도 하였다[1]. 이와 같은 문제 해결을 비롯해 유비쿼터스 기술의 발전은 수집된 정보를 무선주파수를 이용하여 단순 교환하는 수준에서 무선센서 네트워크(WSN:Wireless Sensor Network)를 통해 다양한 정보 교환이 가능해졌고, 나아가 유비쿼터스 센서 네트워크(USN:Ubiquitous Sensor Network)와 센싱 기술이 접목되면서 사물간의 정보교환은 물론 사물과 인간까지도 정보교환이 가능한 사물인터넷(IoT: Internet of Things)으로 발전하였다[2]. IBM은 지금의 사물인터넷 수준은 1.0, 2.0단계를 지나 3.0단계에 있다고 한다. 또한 3.0단계로 진입하면서 가정 내 스마트 홈서비스를 비롯한 정부의 에너지 관리시스템, 환자의 안전을 위한 응급서비스 등으로 서비스의 폭이 넓어지면서 관련 제품 및 서비스로 인한 보안에 대한 대처문제도 복잡 다양해지고 있음을 강조하였다[3]. 김학용(2019)은 사물인터넷의 경우 인터넷 보안에서는 존재하지 않았던 다양하고 새로운 보안문제가 발생할 것이라는 전망을 내놓았다[4]. 복잡 다양해지고 있는 보안문제 대처를 위해 국내의 경우 KISA(한국인터넷진흥원)의 IoT보안인증기준에 따라 IoT제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족 시 인증서를 발급해주고 있다. 따라서 본 연구에서는 사물인터넷 시장의 성장에 따른 보안관련 서비스 향상을 위해 AHP분석을 통해 현재 KISA의 IoT보안인증기준 평가항목 중에서 평가 중요도 순위를 도출함으로써 평가비중을 어디에 두어야 할지를 결정하는데 도움이 되고자 한다. 연구의 기대효과에 있어서는 사물인터넷제품의 자율적 보안강화를 유도할 수 있고 국내 사물인터넷기업 보안역량 강화 및 해외진출 활성화에 기여할 수 있으며, 사물인터넷제품에 대한 국민의 불안감 해소와 같은 효과를 기대할 수 있겠다.

II.이론적 배경

1. 사물인터넷과 보안

사물인터넷은 1999년 미래 사회의 전망으로 미국 MIT대학 케빈 애슈턴(Kevin Ashton)이 사물인터넷이라는 용어를 처음 사용한 후 닉 웨인라이트(Nick Wainwright)에 의해 물리적 대상물인 제어기, 센서, 액추에이터와 데이터 네트워크 및 서비스를 통합하는 기술로 정의되고 있다[5]. 사물인터넷구성은 3단계로 이루어져 있다. 첫 번째 단계는 기존의 단순 디바이스가 아닌 데이터 수집이 가능한 센스와 Sink Nodse가 결합된 형태의 단계이다. 두 번째 단계는 모아진 데이터를 서비스하기 위한 각종 Gateway Nodes 즉, 단말기가 되겠다. 마지막 단계에 있어서는 다양한 의미로 설계된 서비스 개념이 단말기와 연결되어 사물인터넷 서비스가 이루어는 단계이다[6]. 이처럼 사물인터넷 서비스를 위해서는 센싱 기술의 역할이 매우 중요하다. 최근 일본 도쿄공업대 야마네 다이스케 교수 연구팀이 제안한 두 개의 칩으로 구성된 새로운 미세전자기계 에너지 수확기(Micro Electromechnical Energy Harvester)가 관심을 모으고 있다. 연구팀이 제안한 내용을 정리하자면 사물인터넷에 연결되는 모든 기기를 구동하기 위해서는 에너지 공급이 필수적이다. 이러한 에너지 공급의 효율성 및 응용장치 설계의 유연성 확보를 위해 [그림 1]에서 보듯이 기존의 MEMS는 전체시스템에 하나의 칩을 포함한 일렉드릿 기반 MEMS 에너지 수확기인 관계로 설계에 있어서 일렉트릿과 MEMS 구성품의 제작과정이 양립되어야 하는 제한 요소가 있었다. 야마네 연구팀은 이러한 문제 해결을 위해 일렉트릿과 MEMS 가변축전지에 칩을 분리하여 포함함으로서 MEMS 구성품 설계제작의 용이성은 물론 에너지 수확의 극대화하는 새로운 MEMS를 발표하였다[7]. 이 같은 기술의 발전이 중요한 이유는 영화와 같은 사물인터넷 시대를 열어 가는데 기폭제 역할을 하게 될 극소형 센서 개발의 자율성을 부여하는 원동력이 될 주요한

기술이기 때문이다. 그리고 Clair Rowland(2015) 등은 사물인터넷 디바이스 설계에 있어서 디바이스의 기능 구성, 일관성, 연속성을 강조하였다[8]. 여기에는 디바이스 기능분배 및 사용자인터페이스를 고려한 다양한 요소가 복합적으로 작용되어야 함을 의미하는 인터유저빌리티 개념이 추가되어야 한다[9].

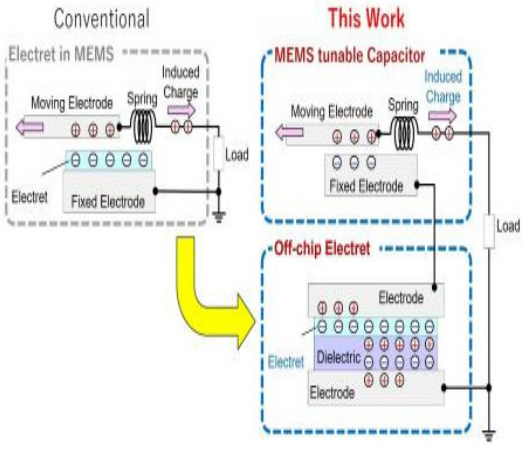

그림 1. MEMS Vibratory Electret Harvester

사물인터넷 기술의 발전과 더불어 사물인터넷 시장의 활성화를 위해서는 보안 기술이 매우 중요하다. 사물인터넷이 4차 산업혁명의 뜨거운 이슈로 부각되면서 관련 보안 기술에 대한 연구에도 박차가 가해지고 있다. 사물인터넷 보안에 대한 기술적 문제는 기존의 인터넷 보안 대처기술 수준을 넘어 사물인터넷을 통해 새롭게 등장하는 보안 위협에 대한 대처기술을 의미하기도 한다. 무엇보다 보안 위협에 대한 미흡한 대처기술 수준으로 인한 사이버범죄 및 테러가 확산되면서 사이버전쟁까지도 발생하고 있다는 사실이다. 사물인터넷 보안은 장봉임(2014)의 주장처럼 사물인터넷을 구성하고 있는 애플리케이션, 네트워크, 단말기와 같은 구성요소별 보안위협에 대한 대처기술을 의미한다[10]. 사물인터넷 시장을 선점하기 위해 삼성을 비롯한 구글, 시스코와 같은 세계적인 기업들이 500억개 이상으로 늘어날 사물인터넷 디바이스에 영향을 미칠 수 있는 기술, 표준, 플랫폼 개발에 열을 올리고 있다[11]. 특히 플랫폼은 매우 중요한 위치에 있으며 정보나 서비스 교환을 위해 다양한 플랫폼이 만들어 졌으나 독자적인 개발에 의해 구축된 플랫폼 간 호환은 어려운 실정이다. 이러한 문제해결을 위해 이종 사물인터넷 플랫폼 간 인터워킹을 위한 연구로는 김재호 등[12]에 의한 OCI(Open Interconect Consortium)와 같은 사물인터넷 인터워킹 표준기술에 대한 소개를 비롯해, 이동규 등[13]이 CoAP(Constrained Application Protocol)와 같은 프로토콜을 DDS(Data Distribution Service)로 바인딩 하여 인터워킹을 수행하는 등의 많은 연구 결과가 있지만 아직 미흡한 실정이다. 문제는 현재로서 인터워킹이 수행되어도 보안위협에 대한 대처가 어렵다는 사실이다. 이러한 문제해결에 접근하기 위해 오세라 등은 보안요구사항 중에 이종 사물인터넷 플랫폼 간 인가, 인증 수행을 위한 FIWARE와 oneM2M 사물인터넷 플랫폼 간 KeyRock과 클라이언트 등록이 된 요구에 대해 OAuth 2.0을 통해 토큰을 발급받아 KeyRock과 AuthZForce에 의해 토큰의 검증을 위한 모든 절차가 이루어지면 Wilma가 디바이스에 인증, 인가의 결과를 반환하는 OAuth 2.0기반의 [그림 2]와 같은 이종 사물인터넷 플랫폼 간 정보 및 서비스 교환이 가능한 보안 프레임 워크를 제안하였다[14]. 그리고 기술관점에서 몇 가지 더 보완하자면 서비스과부하, 컴퓨팅, 저장문제 해결을 위한 클라우드 시스템에 대한 시스템적 문제 제고, 블록체인과 같은 해킹에 대한 리스크를 감소시키기

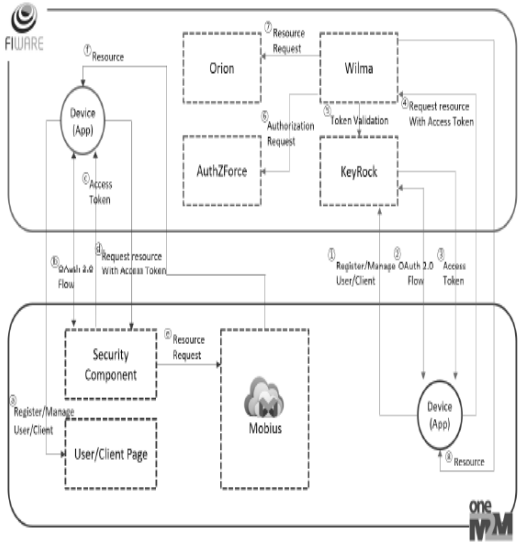

그림 2. Detailed Flow of FIWARE-oneM2M Secure Interworking

위한 보안솔루션 개발에 필요한 신기술 도입문제, 마지막으로 보안위협 발생에 따른 법적 제도 마련을 들 수가 있다[15].

2. 사물인터넷 보안인증서비스

사물인터넷 세계 시장 규모에 대해 경제적 부가가치 측면에 있어서 Gartner그룹은 2020년 1.9조 달러에 달할 것으로 전망하였다[16]. CISCO는 IoT기기의 경우 2014년에 144억 개 이었던 것이 2020년에는 501억 개로 증가할 것으로 예상하였으며, 미국 시장조사업체IDC는 사물인터넷 시장의 규모를 2013년 1조 9천억 달러에서 2020년 7조 1천억 달러로 증가할 것이라는 분석결과를 내놓았다[17]. 그리고 국내의 경우 전해영(2016)의 자료에 의하면 2013년 2조 3,000억원에서 2020년에는 17조 1,000억원으로 7.5배가량 증가할 것이라는 자료를 내놓았다[18].

이러한 성장세와 더불어 최근 보안 IP카메라, 셋톱박스 등 사물 인터넷기기가 리눅스 달 로즈 웜으로 인해 감염된 사례가 미국에서 발생하면서 사물인터넷 보안 정책의 한계를 비롯한 보안 위협요소의 증가, 개인정보 침해 사례가 급증하면서 보안관련 사물인터넷 기술적 문제가 우려되고 있다[19].

이와 같은 보안문제를 둘러싼 복잡한 환경 속에서 사물인터넷의 효과적인 서비스를 위해서는 보안 위협에 효과적으로 대처하기 위한 보안인증서비스 인증기준 평가항목 결정이 중요하다. 먼저 보안위협에 따른 보안인증서비스 인증기준 평가항목 결정을 위해서는 사물인터넷의 보안 요구사항에 대한 정리가 필요하다. Borgia(2014)는 사물인터넷 보안 요구사항에 대해 비밀성, 무결성, 입증성, 권한부여, 결합성 그리고 사생활 보호 등에 대한 데이터보안이 전제가 되어야 한다고 주장하였다[20]. 사물인터넷 전체적인 요구사항에 대해 오세라 등은 이종성, 자원 제약성, 동적 환경 등과 같은 사물인터넷의 기본적인 특성에 따른 플랫폼, IoT 네트워크, 서비스, 공격자, 사용자, 클라우드와 같은 요소를 포함하여 고려되어져야 한다고 주장하였다[21]. 보안요구사항의 동향에 대해 황인태 등은 보안표준요구사항으로 기밀성, 무결성, 가용성, 부인방지, 인증, 인가와 같은 범주를 도출하고 결론에 있어서 보안요구사항 범주 중에 기밀성, 무결성, 인증, 인가가 주로 활용되고 가용성과 부인방지는 크게 이슈가 되지 않고 있다고 정리하였다[22]. 결과적으로 높은 수준의 보안인증을 받기 위해서는 기밀성, 가용성, 무결성, 인증, 인가와 같은 보안요구사항에 대한 사물인터넷 기기의 기술적 구현이 가능해야한다[23]. 이와 관련해서 장봉임(2014)은 사물인터넷을 구성하고 있는 요소별로 발생할 수 있는 데이터 위변조, 데이터의 기밀성, 무결성, 프라이버시 침해, 비 인가된 서비스 및 사용자 접근, 인증방해, 정보유출, 서비스 거부, 복제공격 등과 같은 보안위협에 대한 대처 기술이 중요하다고 주장하였다[10]. 그리고 로컬 및 원격 통신의 암호화 문제, 평문저장장치, 원격 시스템 접속문제, 직렬연결접속으로 인한 무단접속 문제와 같은 보안상 취약점도 함께 해결되어져야 한다[24]. 이처럼 안정적인 보안인증 서비스가 이루어지기 위해서는 사물인터넷관련 보안위협에 대한 보안 요구사항의 정리 및 기술적 구현 가능여부가 매우 중요하다. 이와 같은 문제해결을 통해 보안인증서비스 인증기준이 마련된다면 안정적인 사물인터넷 시장 성장에 도움이 될 것이다. 따라서 적실성 있는 인증기준 결정 위해서는 어떤 인증기준 평가항목에 우선순위를 두어야 할지에 대한 근거가 필요하다고 사료되며, 이러한 근거 도출에 필요한 연구결과가 보안인증서비스 인증기준 결정에 반영된다면 보다 완성도 높은 보안인증서비스 인증기준이 마련될 것으로 판단됨.

Ⅲ. 연구설계

1. 연구모형

본 연구는 사물인터넷(IoT) 보안인증 기준 항목들에 대한 상대적 중요도 우선순위를 분석하기 위해 KISA 한국인터넷진흥원의 IoT보안 시험인증 기준에 대한 분류를 토대로 평가항목들을 선정하였으며 연구모형은 다음의 [그림 3]과 같다[25].

그림 3. 연구모형

2. AHP 평가기준 및 평가항목

본 연구를 위한 계층 1의 평가기준 및 평가항목과 계층 2의 평가항목에 대한 평가내용은 다음의 [표 1]과 같다.

표 1. 평가기준 및 평가항목 설명

평가기준		평가항목	설명
계층 1	보안인증기준	인증	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구
		암호	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용
		데이터보호	제품 간 전송되는 중요정보는 암호화
		플랫폼보호	보안취약점 존재여부를 확인하고 제거
		물리적보호	비인가자의 내부 포트 접근을 방지
계층 2	인증	사용자인증	사용자 신원을 검증하기 위해 식별인증
		인증정보 안전한사용	인증정보의 보안을 위해 인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 되고 비밀번호입력 시 마스킹처리, 인증 실패 시 실패사유에 대한 피드백 정보 제공안함
		제품인증	하드웨어 제품은 고유 식별정보를 보유해야 하며 제품 간 중요정보 전송 시 제품제어를 위한 상호연결 수행 시 상호인증
	암호	안전한 암호 알고리즘 사용	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용
		안전한 키 관리	암호키는 안전성이 검증된 방법으로 생성·갱신·분배·사용·저장·파기
		안전한 난수 생성	난수 생성 시 난수성이 검증된 알고리즘을 이용
	데이터보호	전송/저장 데이터 보호	제품 간 전송되는 중요정보의 암호화와 안전한 보안 모드를 사용해서 통신채널 생성해야하며 제품에 저장되는 중요정보는 암호화하며 사용자 필요에 의해 제품에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵게함
		정보흐름 통제	허가되지 않은 네트워크 트래픽 차단 기능을 제공
		안전한 세션관리	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 하며, 세션 ID는 예측할 수 없는 값
		개인정보 보호	제품에서 처리하는 개인정보는 비식별화 조치
	플랫폼보호	소프트웨어 보안	시큐어코딩 적용, 보안취약점 존재여부 확인 후 제거, 소스코드 분석 방지를 위한 난독화 적용, 주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원
		안전한 업데이트	업데이트 수행 전 인가된 사용자 여부를 확인하며 업데이트 실패 시 롤백기능을 지원, 업데이트 수행 전 무결성을 검사
		보안관리	불필요한 서비스는 제거하거나 비활성화, 원격관리는 신뢰할 수 있는 환경에서 수행, 최신 보안패치 적용된 버전의 라이브러리, 하드웨어 및 소프트웨어의 자체 시험 기능을 제공
		감사기록	보안과 관련된 이벤트는 감사기록을 생성해야 하며, 감사기록에 대한 보호 기능을 제공
		타임 스탬프	신뢰할 수 있는 타임스탬프 기능을 지원해야 함
	물리적보호	물리적 인터페이스 보호	불필요한 외부 인터페이스는 비활성화, 필요 시 접근통제 기능을 지원해야 하며, 비인가자의 내부 포트 접근을 방지
		무단조작 방어	비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원

Ⅳ. 실증분석

1. 연구도구의 개발

본 연구의 분석은 Saaty(1990)의 전문가를 대상으로 설문하여 분석하는 계층적의사결정 분석을 실시하였으며, 응답자의 편의를 돕기 위해 각 평가항목에 대한 구체적인 설명을 함께 제시하였다[26]. 계층의사결정과정은 설문대상이 연구와 부합되는 전문가들의 의견을 반영하여 평가하는 것이 매우 중요하다. 이에 따라 설문지의 평가항목은 한국인터넷진흥원(KISA)의 IoT보안인증서비스 평가항목을 근간으로 하였으며, 보안인증관련 연구자와 전문가들의 협의를 통해 평가항목들에 대한 중요도를 측정하였다.

2. 자료의 수집

본 연구를 위한 AHP설문은 2019년 3월부터 4월초까지 보안인증관련 담당자를 대상으로 12부의 설문을 배부하여 총 10부의 설문을 회수하였다. 분석을 위해 AHP 응답에 대한 조사결과는 Expert Choice 2000을 적용하였으며, 인구통계적 특성은 SPSS 20.0을 적용하였다.

먼저, AHP 설문은 응답자가 일관성을 가지고 평가항목에 응답했는지 검증하기 위해 일관성 지수(CI; Consistency Index)값을 계산하여 응답의 신뢰성을 검토한다. 일반적으로 응답자가 전문성이 높을수록 낮은 값을 유지하며, 응답자의 설문에 대한 일관성의 기준은 CI 값이 0.1 이상이 나오면 응답을 신뢰할 수 없다고 판단한다[27]. 본 연구에서는 CI값이 0.1를 초과한 1명의 의견은 최종분석에서 제외하였다.

최종분석에 사용된 설문응답자의 특성을 살펴보면, 인증컨설턴트 3명, 보안구축담당자 4명, 보안인증기관 담당자 2명으로 나타났다. 정보보호 관련 업무경력은 5년 미만 1명, 10년 미만 7명, 15년 미만 1명이었다. 다음으로 현재 IoT보안인증서비스 평가항목기준의 선정항목들이 적합한 수준이라고 판단하는지에 대한 전문가들의 의견들은 아래의 [표 2]와 같다.

표 2. IoT보안인증서비스 평가항목 기준

구분	인원 (명)
현재 IoT보안인증서비스(IoT-SAP) 평가항목 기준이 적합한 수준이라고 판단	8
현재 IoT보안인증서비스(IoT-SAP) 평가항목 기준이 적합하지 않은 수준이라고 판단	1

3. AHP 분석결과

본 연구를 IoT보안인증서비스 평가항목 요인의 중요도 우선순위 분석을 위한 AHP 분석결과는 다음과 같다. 1계층의 우선순위를 분석한 결과 [표 3]과 같이 데이터보호 항목이 중요도 0.343으로 가장 높게 나타났으며 2순위도는 암호 항목이 중요도 0.222로 나타났다. 플랫폼보호, 물리적보호, 인증은 각각 중요도 수치가 0.197, 0.165, 0.073으로 나타났다.

표 3. IoT보안인증서비스 평가항목 1계층 결과

계층1	중요도	우선순위
인증	0.073	5
암호	0.222	2
데이터보호	0.343	1
플랫폼보호	0.197	3
물리적보호	0.165	4
CI	0.01	

다음으로 2계층의 IoT보안인증서비스 평가항목을 분석한 결과, 아래의 [표 4]와 같이 인증항목에서는 사용자인증을 중요하게 판단하고 있었고 암호항목에서는 안전한 키관리를 우선적으로 중요하게 생각하고 있었다. 데이터보호항목에서는 개인정보보호가 우선시 되어야 하고, 플랫폼보호에서는 보안관리가 중요하게 나타났으며, 물리적보호항목에서는 무단조작방어의 중요도가 높게 나타났다.

표 4. IoT보안인증서비스 평가항목 2계층 결과

계층1	계층2	CI	중요도	순위
인증	사용자인증	0.01	0.373	1
	인증정보의 안전한 사용		0.277	3
	제품인증		0.351	2
암호	안전한 암호알고리즘 사용	0.02	0.293	3
	안전한 키 관리		0.367	1

	안전한 난수생성		0.340	2
데이터 보호	전송/저장 데이터 보호	0.01	0.112	4
	정보흐름 통제		0.167	3
	안전한 세션 관리		0.181	2
	개인정보보호		0.540	1
플랫폼 보호	소프트웨어보안	0.08	0.149	4
	안전한 업데이트		0.111	5
	보안관리		0.264	1
	감사기록		0.219	3
	타임스탬프		0.257	2
물리적 보호	물리적 인터페이스 보호	0.00	0.353	2
	무단 조작 방어		0.647	1

다음으로 각 계층별 항목의 총제적인 평가항목의 중요도를 평가한 결과는 다음의 [표 5]와 같이 데이터보호항목의 개인정보보호가 가장 중요하게 판단되어야 하는 항목으로 나타났으며 다음으로 물리적보호항목에서 무단조작방어가 중요하며 암호에서는 안전한 키 관리의 평가가 중요한 항목으로 도출되었다.

표 5. IoT보안인증서비스 평가항목 최종우선순위 결과

계층1	계층2	최종 중요도	최종 우선순위
인증	사용자인증	0.027	14
	인증정보의 안전한 사용	0.020	17
	제품인증	0.026	15
암호	안전한 암호알고리즘 사용	0.065	5
	안전한 키 관리	0.081	3
	안전한 난수생성	0.075	4
데이터보호	전송/저장 데이터 보호	0.038	12
	정보흐름 통제	0.057	8
	안전한 세션 관리	0.062	6
	개인정보보호	0.185	1
플랫폼보호	소프트웨어보안	0.029	13
	안전한 업데이트	0.022	16
	보안관리	0.052	9
	감사기록	0.043	11
	타임스탬프	0.051	10
물리적보호	물리적 인터페이스 보호	0.058	7
	무단 조작 방어	0.107	2

V. 결론

사물인터넷 보안인증을 위해 한국인터넷진흥원이 전반적인 보안인증 업무수행을 하고 있으며, IoT보안인증은 IoT제품과 제품의 구성요소 기능단위 모듈, IoT제품 관리 등의 목적으로 IoT제품과 연동하는 모바일 앱을 대상으로 시행하고 있다.

본 연구는 IoT보안인증 기준유형에 나온 항목들을 토대로 중요하게 관리되어서 평가받아야 하는 항목들을 보안인증관련 전문가를 대상으로 설문을 수행하여 우선순위 항목들을 도출하였다. 본 연구의 분석결과 IoT보안인증 서비스 평가항목의 중요도 최종우선순위에서 데이터보호 항목의 개인정보보호가 가장 높은 항목으로 도출되었다. 이는 IoT제품 간 전송되는 중요정보는 암호화하여 적용되는데 제품에서 처리하는 개인정보는 비식별화 조치되어지기에 관리적차원의 개인정보보호의 관점에서의 데이터보호가 강조되어야 한다는 부분을 판단한 것이다. 다음으로 물리적보호의 무단조작방어의 중요성이 높게 도출되었다. 이는 비인가자의 내부포트 접근을 물리적으로 방어하는 것이 중요하며 비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원하는 것은 IoT보안의 기술적인 부분에서도 보다 강화되어야하는 부분임을 강조한다.

반대로 IoT보안인증서비스 평가항목에서 가장 낮게 나타는 항목은 1계층의 인증항목으로 도출되었다. IoT제품이 위협으로부터 안전성을 확보하기 위한 기본적인 요건자체가 보안인증 항목에 포함되어있는 사용자인증, 인증정보의 안전한 사용, 제품인증은 보안내재화를 위해 필수적으로 강화되어 있다는 전제하에서 인증대상에 대한 평가를 받고 보안인증을 발급해야 하는 것은 필수적인 사항이기에 상대적으로 낮은 중요도를 나타낸 결과라고 해석되어 질 수 있다.

본 연구에서는 한국인터넷진흥원이 IoT기기를 대상으로 보안인증 서비스를 제공하고 있는 상황에서 보다 안전한 IoT기기 보급을 위해 제조사가 최소한의 보안인증인 LITE 등급과 국제 표준 수준의 보안인증 항목인 STANDARD등급에 맞추어 제품개발을 할 때 우선적으로 중요하게 반영할 수 있는 항목들을 제시하였다는데 실무적인 의의가 있다. 또한 중요도가 높게 평가된 항목들을 활용하여 보다 강화해야 하는 보안인증 가이드라인의 설계에 반영할 수 있는 실무적인 틀을 제공하는데 의의가 있다.

본 연구의 한계점과 향후 연구방향은 다음과 같다. 먼저, 본 연구는 보안인증관련 전문가를 대상으로 설문을 수행하여 최종적인 항목의 우선순위항목들을 도출하였다. 추후 연구에서는 보안인증관련 전문가들 중에서 업무역할에 따른 전문가들을 대상으로 비교·분석하는 연구를 수행해야 할 것이다. 또한 IoT보안인증서비스 평가항목사항들에 대한 기준을 기업의 특성관점에서 평가받을 수 있는 항목들로 구분하지 않았다. 향후 연구에서는 기업의 특성 및 정책사항에 따른 기준항목들을 개발하는 연구를 할 필요성이 있다.

참 고 문 헌

[1] 김진영, "사물인터넷 활성화를 위한 입법과제 및 개선방안 연구," 과학기술법연구, 제24권, 제1호, pp.43-92, 2018.

[2] 주대영, 김종기, "초연결시대 사물인터넷(IoT)의 창조적 융합 활성화 방안," 서울: KETI 산업연구원, pp.32-34, 2014,

[3] 이강윤, 이정훈, 정창우, 탁영주, "사물인터넷: IoT 3.0과 사물인터넷 플랫폼 기술," 정보처리학회지, 제21권, 제2호, pp.5-6, 2014.

[4] 김학용, "2019년 사물인터넷 시장 전망," daum brunch, 2019년1월4일 기사 재구성.

[5] 전홍배, "사물인터넷 기술의 개념, 특징 및 전망," Entrue Journal of Information Technology, 제1권, 제1호, pp.7-19, 2015.

[6] 한국인터넷진흥원, Op.cit., pp.3-4, 재구성

[7] 김병희, "사물인터넷 가속화 이끈다," The Science Times, 2019.3.24. 기사 재구성.

[8] Clair Rowland, Elizabeth Goodman, Martin Charlier, Ann Light&Alfred Lui., "Designing Connected Products: UX for the Consumer Internet of Things," O'Reilly Media, pp.9-11, 2015.

[9] 안미경, *IoT 환경에서 인터유저빌리티(Interusability) 개선을 위한 사물성격(Personality of Things)중심의 UI 프로토타이핑에 대한 연구,* 서울여자대학교 대학원, 석사학위논문, pp.1-110, 2018.

[10] 장봉임, 김창수, "사물인터넷 보안기술 연구," 보안공학연구논문지 Journal of Security Engineering, 제11권, 제5호, pp.429-438, 2014.

[11] Cisco, "The Internet of Things"[Internet], https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[12] J. H. Kim, S. C. Choi, N. M. Sung, and J. S. Yun, "Standard Interworking Technologies for Internet of Things," The Journal of The Korean Institute of Communication Sciences, Vol.33, pp.55-64, 2016.

[13] D. G. Lee, D. H. Kim, and T. M. Chung, "A Proposal for a Method of Interworking with DDS on IoT Platforms," Proceedings of Symposium of the Korean Institute of Communications and Information Sciences, Vol.60, pp.385-386, 2016.

[14] 오세라, 김영갑, "이종 사물인터넷 플랫폼 간 보안 상호운용을 위한 프레임워크," 정보처리학회논문지/컴퓨터 및 통신 시스템, 제7권, 제3호, pp.81-90, 2018.

[15] 정태진, 이광민, "IOT(사물인터넷) 보안과 국제범죄 대응방안," 한국경찰학회보, 제19권, 제5호, pp.256-278, 2017.

[16] https://www.gartner.com/doc/2625419?ref=mrktg-srch, Retrieved on Sep. 09, 2018 재구성.

[17] https://donghoson.tistory.com/166, 자료 재구성.

[18] 전해영, "사물인터넷(IoT) 관련 유망산업 동향 및 시사점," VIP REPORT, pp.16-24, 2016.

[19] 이동혁, 박남제, "안전한 IoT 환경을 위한 기술 및 정책적 사후 보안관리 프레임워크," 한국정보기술학회논문지, 제15권, 제4호, pp.127-138, 2017.

[20] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, Vol.54, pp.1-31, 2014.

[21] S. R. Oh and Y. G. Kim, "Security Requirements for Internet of Things," IEEE 2017 Platform Technology and Service(PlatCon), pp.1-6, Feb. 2017.

[22] I. T. Hwang and Y. G. Kim, "Analysis of Security Standardization for the Internet of Things," IEEE 2017 Platform Technology and Service (PlatCon), pp.1-6, Feb. 2017.

[23] 고재용, 이상길, 김진우, 이철훈, "IoT보안 요구사항

및 보안 운영체제 기반 기술 분석," 한국콘텐츠학회논문지, Vol.18 No.4, pp.164-177, 2018.
[24] 김미희, "사물인터넷(IoT)환경에서 프라이버시 보호 기술: 네트워크 카메라 사례 연구," 한국콘텐츠학회논문지, Vol.16 No.9, pp.329-338, 2016.
[25] 한국인터넷진흥원, *IoT제품 대상 보안인증 적용 기준*, 2019.
[26] J. G. Yoon, "A Comparison of 3 Statistical Technique for Evaluation MIS Sucess Factor = Application Efeects and Limitations of AHP as a Research Methodology," Journal of the Korean Operations Research and Management Science Society, Vol.21, No.3, pp.109-124, 1996.
[27] O. S. Vaidya and S. S. Kumar, "Analytic hierarchy process: An overview of applications," European Journal of Operational Research, Vol.169, pp.1-29, 2004.

저 자 소 개

강 다 연(Da-Yeon Kang) 정회원

- 2006년 2월 : 한국해양대학교 해운경영학과(경영학사)
- 2008년 2월 : 부산대학교 경영학과(경영학석사)
- 2014년 8월 : 한국해양대학교 해운경영학과(경영학박사)
- 현재 : 경북대학교 경영학부 BK21 플러스 Post-Doc

〈관심분야〉 : 정보시스템 보안관리, 보안정책관리, 항만물류보안, 데이터마이닝, 기업경영분석, AI, IoT, ICT, 정보기술융합

황 종 호(Jong-Ho Hwang) 정회원

- 1994년 2월 : 일본 TAKUSHOKU대학교 상학과(경영학사)
- 1996년 2월 : 일본 TAKUSHOKU대학교 상학연구(경영학석사)
- 1999년 10월 : 일본 TAKUSHOKU대학교 상학연구(경영학박사)
- 2000년 2월 ~ 현재 : 동명대학교 경영정보학과 교수

〈관심분야〉 : 정보시스템 보안관리, 데이터베이스, 경영자료분석, 데이터마이닝, 비즈니스특허모델